УДК 327

Булавин Алексей Владимирович

**соискатель кафедры международных отношений
Нижегородского государственного университета им. Н.И. Лобачевского**

О ПОДХОДАХ США И КИТАЯ К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Аннотация:
В статье автор рассуждает об угрозах информационной безопасности, в том числе имеющих стратегический характер, исходящих из киберпространства. Проводится анализ подходов специалистов США и Китая к противодействию данным угрозам, а также форм и методов, необходимых для решения этих задач. Также рассматривается вопрос о правомерности объявления киберпространства зоной боевых действий, и дан ответ на этот вопрос с точки зрения трех уровней ведения боевых действий: стратегического, оперативного и тактического.

Ключевые слова:
Китай, критическая инфраструктура, кибербезопасность, киберпространство, дипломатия, электронное правительство, США, боевые действия.

Bulavin Alexey Vladimirovich

**PhD applicant,
International Relations Department,
Nizhny Novgorod State University**

CONCERNING APPROACHES OF THE USA AND CHINA TO CYBERSECURITY

Summary:
The article discusses existing cybersecurity risks, including the strategic ones originated from the cyberspace. The author analyzes approaches of the experts from the USA and China to the cyber threats control, as well as forms and methods of appropriate countermeasures. The author also considers a question, if it is rightful to treat the cyberspace as a combat zone, and answers this question from three perspectives: strategic, operation, and tactic.

Keywords:
China; United States; critical infrastructure; cybersecurity; cyberspace; diplomacy; e-government; warfare.

С точки зрения национальной безопасности, с киберпространством связаны две основные угрозы: кибершпионаж и кибератаки. Противоборство в киберпространстве рассматривается специалистами по аналогии с военными действиями на трех уровнях: тактическом, оперативном и стратегическом. Тактический уровень противоборства в киберпространстве – это «рутинная», ежедневная деятельность, заключающаяся в попытках хищения информации и атаках на компьютерные системы рядовых граждан, фирм и компаний. Оперативный уровень предполагает крупномасштабные атаки, такие как ДоС-атаки на Bank of America и другие банки или применение вируса Stuxnet в Иране. На данном уровне противоборства в киберпространстве можно спровоцировать социальное недовольство внутри страны (как в случае с Эстонией в 2007 г., пострадавшей от действий хакеров), а также рост напряженности в отношениях между странами – по мере того как накапливаются свидетельства того, что ряд стран создает и использует средства неправомерного доступа к компьютерной информации. На тактическом и оперативном уровнях противоборство в киберпространстве становится предметом юридического внимания и требует внедрения единообразной терминологии и исследования с точки зрения права.

Стратегический уровень противоборства в киберпространстве фактически означает ведение реальных военных действий. Отличие от предыдущих уровней заключается в долгосрочных, более разрушительных последствиях, когда целью атак становится вывод из строя инфраструктуры противника, нанесение человеческих потерь, нарушение связи, существенные экономические потери. В США данный вид кибервойны будет нуждаться в получении одобрения со стороны Конгресса.

Западные эксперты выдвигают три необходимых условия защиты от кибератак: устойчивость систем, способность распознать принадлежность атакующего, возможность ответных наступательных действий. Создание устойчивых систем серьезно сдерживается отсутствием единых технических стандартов и недостаточным уровнем совместимости действующих систем [1, p. 45–58]. В этой связи возникает вопрос возможности принудительного внедрения таких стандартов и его механизмов. Отдельные американские специалисты выдвигают идею создания международного органа по решению проблем кибербезопасности, который привлекал бы лиц, ответственных за выработку решений из государственных и частных структур, для разработки единых стандартов и создания соответствующих мощностей. Кроме того, предлагается возможность внедрения международных санкций в киберпространстве против лиц или группировок, осуществляющих кибератаки против США [2].

В данном контексте существенный научный и практический интерес представляет анализ подходов китайских специалистов к вопросам обеспечения кибербезопасности. Следует отметить, что в настоящее время подход Китая к обеспечению информационной безопасности существенно противоречит американскому пониманию открытости в Интернете [3, с. 130–134]. Цель контроля над Интернетом в Китае – предотвратить проникновение нежелательной информации внутрь страны и утечку чувствительной информации за рубеж, в том числе путем блокирования основных социальных сетей и поисковых систем. Вместе с тем западные эксперты высказывают мнение, что Китай и США все же имеют общие точки соприкосновения в сфере информационной безопасности в связи с ростом киберпреступности на территории Китая. При этом Пекин особенно волнует возможность кибератак террористов на ключевые объекты инфраструктуры. Однако эксперты отмечают различие в терминологии, которое в свою очередь иллюстрирует различные подходы двух стран к проблеме. Если в США наиболее употребительным является термин «кибербезопасность» (cybersecurity), относящийся преимущественно к обеспечению безопасности архитектуры Интернета, то в Китае (так же, как в России) используется термин «информационная безопасность», предполагающий ограничения на распространение нежелательной информации. Разница в целях и подходах затрудняет диалог между США и Китаем.

В самом Пекине присутствуют различные точки зрения на выработку общемировых стандартов безопасности в компьютерной сфере. Лица, ответственные за принятие политических решений в центральном руководстве страны, обеспокоены долгосрочной перспективой формирования технологической зависимости Китая от западных стран. Их стратегия достижения независимости базируется на внедрении собственных технологических инноваций и создании конкуренции американским компаниям. В соответствии с имеющимися планами, к 2020 г. расходы на НИОКР должны составить 2,5 % ВВП, а к 2049 г. Китай планирует занять лидирующее положение по внедрению инноваций. Этому способствуют имеющиеся в его распоряжении существенные людские ресурсы: более чем из шести миллионов выпускников ежегодно около 60–70 % составляют научно-технические специалисты и инженеры. Вместе с тем китайская политика внедрения инноваций имеет и противозаконную составляющую – речь идет прежде всего о хищениях интеллектуальной собственности. Китай допускает это, поскольку располагает соответствующими возможностями при минимальных рисках.

С военной точки зрения Китай рассматривает себя как более слабую державу по сравнению с США, что вынуждает его вырабатывать стратегию асимметричного ответа. В качестве одного из элементов такой стратегии может быть вмешательство в целях противоракетной обороны в систему управления спутниками и в другие элементы американ-

ского киберпространства. Кроме того, Китай активно использует противоборство в киберпространстве в целях решения внутренних проблем. В частности, хакерским атакам и спам-рассылкам подвергаются ресурсы тибетских активистов и «мозговые центры», занимающиеся проблемами Тибета.

Если контроль над Интернетом в понимании США должен быть прозрачен и осуществляться значительным числом участников (в том числе с применением научного подхода), то для Пекина в его стремлении в полной мере восстановить государственный контроль над китайским сегментом Сети такой подход неприемлем. Более того, Китай зачастую уличает США в неискренности, обвиняя их в милитаризации киберпространства (путем создания «Электронного командования» – U.S. Cyber Command, а также посредством создания вирусов, подобных червю Stuxnet). Пекин уверен, что разведывательные службы США постоянно присутствуют во внутренних сетях Китая, в том числе через продукцию фирмы Microsoft. Вместе с тем Китай оценивает киберпространство США как более уязвимое по сравнению со своим собственным – именно вследствие жесткого контроля со стороны властей и, как следствие, наличия меньшего количества точек возможного доступа. Кроме того, экономика США в гораздо более значительной мере зависит от киберпространства, нежели экономика Китая.

Следует также отметить, что в Китае отсутствует единая структура, занимающаяся оценкой и анализом получаемых разведсообществом данных (по аналогии с Национальным советом по разведке в США или Комитетами по национальной безопасности США и Великобритании). Как сообщалось, бывший председатель КНР Ху Цзиньтао делал попытку создания подобного ведомства, но оказался неспособен преодолеть нежелание делиться полномочиями со стороны отдельных лиц и целых структур. Ближайшим аналогом являются так называемые ведущие малые группы, занимающиеся целым рядом стратегических вопросов внутренней и внешней политики. Вопросами внешней политики и национальной безопасности занимаются три из них: Центральная малая рабочая группа по внешней политике (Central Foreign Affairs Work Leading Small Group, *zhonguo zhongyang waishi gongzuo lingdao xiaozu*), Ведущая малая группа по вопросам национальной безопасности (National Security Leading Small Group, *zhonguo zhong-yang guojia anquan lingdao xiaozu*) и Ведущая малая группа по проблемам Тайваня (Taiwan Affairs Leading Small Group, *zhongguo zhongyang duitai gongzuo lingdao xiaozu*). Задача указанных групп – организация дебатов между различными группами лиц, ответственных за принятие политических решений, и выработка рекомендаций по ключевым политическим вопросам. Состав малых групп по вопросам внешней политики и национальной безопасности не разглашается, но списки некоторых их участников периодически появляются на некоторых китайско-язычных сайтах. По состоянию на конец 2012 г. в них включали руководителей департаментов пропаганды и международных отношений КПК, министров иностранных дел, обороны, торговли, общественной безопасности и государственной безопасности, бывшего заместителя начальника штаба НОАК (Национально-освободительной армии Китая), а также руководителя подразделения Госсовета КНР по делам Гонконга и Макао [4, p. 45–66].

Поскольку о методах работы указанных малых групп известно крайне мало, можно делать выводы на основе общих тенденций влияния разведки на процесс принятия политических решений. Во-первых, в современном Китае отмечается значительный рост и разделение интересов различных «центров силы» – вплоть до невозможности для ведомств, контролирующих сферы внешней политики и безопасности, эффективно осуществлять свою деятельность. Так, Министерство иностранных дел КНР в большей степени выступает исполнителем, нежели инициатором внешнеполитических действий. Роль

НОАК в процессе принятия решений оценивается как постепенно сокращающаяся. В Политбюро не входят военные руководители высокого уровня, а имеющиеся в составе НОАК структуры не позволяют оказывать существенного влияния на принятие внешнеполитических решений.

Аналогично ситуации на Западе лица, ответственные за принятие политических решений в Китае, не полагаются в полной мере на разведданные. Китайские лидеры, предположительно, в большей степени опираются на альтернативные источники рекомендаций и информации. У каждого из китайских лидеров имеются собственные советники – представители академического сообщества. Источниками информации также служат государственные и частные предприятия, при этом лица, ответственные за принятие политических решений, вынуждены учитывать степень их объективности и заинтересованности [5].

Характеризуя деятельность разведслужб КНР в компьютерной сфере, западные аналитики отмечают, что Китай сравнительно поздно начал использовать возможности Интернета, но достаточно быстро восстановил упущенные позиции. Количество пользователей Интернета возросло с двух миллионов пользователей в 1996 г. (когда у населения КНР впервые появилась возможность доступа к нему) до 538 млн в середине 2012 г. (почти 25 % всех пользователей в мире). НОАК начала учитывать информационные технологии в своих новых стратегических доктринах, а также включила информационный аспект в так называемую «концепцию информационного противоборства». В настоящее время НОАК пытается реализовать концепцию, предусматривающую связь между всеми видами вооруженных сил посредством общей коммуникационной платформы с возможностью доступа к ней на всех уровнях командования.

С начала XXI века была зафиксирована серия компьютерных атак, предположительно имеющих китайское происхождение и направленных против засекреченных правительственных систем и крупных производственных предприятий, а также оппозиционных китайскому правительству групп (таких, как тибетское правительство в изгнании). В докладе компании «Нортроп-Груман», подготовленном для Американо-Китайской комиссии по сотрудничеству в сфере экономики и безопасности, отмечается, что подобные операции являются результатом длительной и тщательной разведработы по изучению сетей, являющихся объектом атаки, а также сетевого анализа с целью поиска уязвимостей и отдельных пользователей с разной степенью удаленности от интересующих объектов. Затем выбранным пользователям осуществляется фишинговая рассылка с последующим распространением «троянов», обеспечивающих удаленный доступ к интересующим ресурсам.

В докладе «Нортроп-Груман» описано разделение труда между группами хакеров, ответственных за обеспечение доступа к системе и извлечение из нее интересующих данных. Основная часть технических мощностей, используемых Китаем для атак на западные оборонные и промышленные системы, находится в распоряжении НОАК и военно-промышленного комплекса Китая. Хотя основные усилия хакеров направлены на сбор чувствительной информации оборонного и научно-технического характера, западные эксперты сходятся во мнении, что в ближайшее время они будут сосредоточены на добывании политической и экономической развединформации, а также сведений о неправительственных организациях и оппозиционных группировках. Последний аспект представляет особенный интерес для министерства государственной безопасности, которое (учитывая неразвитость сотрудничества между разведслужбами Китая), вероятнее всего, развивает соответствующие независимые внутриведомственные возможности.

Кроме того, неясно, насколько эффективно Китай сможет использовать собранные данные. Некоторые высокопоставленные американские военнослужащие характеризуют размах китайского кибершпионажа, направленного против американских госструктур и частного сектора, как «самое крупное перераспределение благосостояния в истории». Однако, по другим оценкам, сложно оценить реальную степень угрозы, которую китайский промышленный шпионаж представляет американским экономическим возможностям. В качестве примеров приводится американская фирма AMSC, согласно заявлениям которой ее китайский партнер – фирма Sinovel незаконно завладела исходным кодом управляющего программного обеспечения AMSC для использования в собственных продуктах, что привело к падению доходности AMSC на 80 %. Другим примером является банкротство канадской телекоммуникационной компании Nortel, ставшей жертвой крупномасштабного промышленного шпионажа со стороны китайской корпорации Huawei. Однако насколько успешным будет дальнейшее копирование Китаем западных технологий в целях обеспечения экономического рывка, зависит во многом от развития китайской экономической модели.

Ссылки:

1. NCAFP. Cyberpower and National Security // American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy. 2013. V. 35. № 1. P. 45–58.
2. Старкин С.В. Аналитические институты разведывательного сообщества США во внешнеполитическом процессе. Н. Новгород, 2011.
3. Старкин С.В. Влияние геополитической среды на трансформацию контрразведывательной парадигмы спецслужб США **//** Вестник Брянского государственного университета. 2011. № 2. С. 130–134.
4. Inkster N. Chinese Intelligence in the Cyber Age // Survival: Global Politics and Strategy. 2013. V. 55. I. 1. P. 45–66.
5. Старкин С.В. Аналитические институты разведывательного сообщества США: концептуальные основы, механизмы и технологии деятельности в условиях глобализации : автореф. дис. … д-ра полит. наук / Нижегородский государственный университет им. Н.И. Лобачевского. Н. Новгород, 2011.

References:

1. ‘NCAFP. Cyberpower and National Security’, 2013, *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy,* vol. 35, no. 1, p. 45–58.
2. Starkin, SV 2011, *Analytical institutions the U.S. intelligence community in the foreign policy process,* Nizhny Novgorod.
3. Starkin, SV 2011, ‘Geopolitical environment impact on the transformation of U.S. intelligence counterintelligence paradigm’, *Bulletin of the Bryansk State University,* no. 2, p. 130-134.
4. Inkster, N 2013, ‘Chinese Intelligence in the Cyber Age’, *Survival: Global Politics and Strategy,* vol. 55, issue 1, p. 45-66.
5. Starkin, SV 2011, *Analytical institutions the U.S. intelligence community: conceptual bases, mechanisms and technology activities in the context of globalization*, D.Phil. thesis abstract, Nizhny Novgorod.